



SNMP-GSH2404L

24+4 Gigabit SNMP Lite Switch

User's Manual





Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

All Trademarks are properties of their respective holders.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN61000-3 and the Generic European Immunity Standard EN55024.

EMC:

EN55022(2003)/CISPR-2(2002)	class A
IEC61000-4-2 (2001)	4K V CD, 8KV, AD
IEC61000-4-3(2002)	3V/m
IEC61000-4-4(2001)	1KV – (power line), 0.5KV – (signal line)

Warning:

- Self-demolition on Product is strictly prohibited. Damage caused by self-demolition will be charged for repairing fees.
- Do not place product at outdoor or sandstorm.
- Before installation, please make sure input power supply and product specifications are compatible to each other.

**Bluetooth®**

© 2009 OvisLink Corporation, All Rights Reserved

Table of Contents

1. Introduction	1
1.1 Overview	1
1.2 How to Use This Guide	1
1.3 Firmware Upgrade and Tech Support	2
1.4 Features	3
2. Installing the SNMP-GSH2404L	4
2.2 Before You Start	4
2.3 Package Content	4
2.4 Optional Accessories	5
2.5 Knowing your SNMP-GSH2404L	6
2.6 Hardware Installation	6
2.6.1 Attaching Rubber Feet	6
2.6.2 Rack-mounted Installation	7
2.6.3 Power On	8
2.7 LED Table	8
3. Configuring the SNMP-GSH2404L	10
3.1 Important Information	10
3.2 Prepare your PC	10
3.3 Management Interface	11
3.4 Introduction to Web Management	11
3.4.1 Getting into Web Management	12
4. Web Management in SNMP-GSH2404L	14
4.1 Menu Structure of SNMP-GSH2404L	14
4.2 Configuration	15
4.2.1 System Configuration	16
4.2.2 Port	20
4.2.3 VLAN Mode Configuration	21
4.2.4 VLAN Group Configuration	25
4.2.5 Aggregation	27
4.2.6 LACP	28
4.2.7 RSTP	30
4.2.8 802.1X	31
4.2.9 IGMP Snooping	39

4.2.10 Mirror Configuration	40
4.2.11 QoS Configuration	41
4.2.12 Filter.....	44
4.2.13 Rate Limit	46
4.2.14 Storm Control.....	47
4.2.15 SNMP	48
4.3 Monitor	50
4.3.1 Detailed Statistics	50
4.3.2 LACP Status	53
4.3.3 RSTP Status	54
4.3.4 IGMP Status	56
4.3.5 Ping Status	57
4.4 Maintenance	59
4.4.1 Warm Restart.....	59
4.4.2 Factory Default	60
4.4.3 Software Upgrade.....	60
4.4.4 Configuration File Transfer	61
4.4.5 Logout.....	62
5. Troubleshooting.....	64
5.1 Incorrect connections.....	64
5.2 Diagnosing LED Indicators	65
5.3 Cabling.....	65
6. Specifications.....	66
7. Network Glossary	69

1

Introduction

1.1 Overview

The SNMP-GSH2404L is a 24-port Gigabit Lite SNMP Managed Switch with 20-Port Gigabit TP slots and 4-Port Gigabit TP/SFP slots. This Switch can be used to build high-performance switched workgroup networks. The switch can be managed through web browser and SNMP agent. In addition, the switch features comprehensive and useful functions such as QoS, Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, IGMP Snooping capability via the intelligent software. It is suitable for SMB applications.

Note:

The switch was for using indoor purpose, if it was used in outdoor environment or connect with cable to outdoor then it must to use a lightning arrester to protect the switch.



1.2 How to Use This Guide

SNMP-GSH2404L is a Lite SNMP managed Switch with many functions. It is recommended that you read through the entire user's guide whenever possible. The user guide is divided into different chapters. You should read at least go through the first 2 chapters before attempting to install the device.

Recommended Reading

Chapter 1: This chapter explains the basic information for SNMP-GSH2404L. It is a must read.

Chapter 2: This chapter is about hardware installation. You should read through the entire chapter.

Chapter 3:

- **3.1 Important Information:** This section has information of default setting such as IP, Username, and Password.
- **3.3 Management Interface:** This section introduces Web management.

- **3.4 Introduction to Web Management:** This section tells you how to get into the WebUI using HTTP.

Chapter 4: This chapter explains all of the management functions via Web management.

Chapter 5: If any trouble in using SNMP-GSH2404L, you can refer to this chapter

Chapter 6: This chapter shows technical specification of SNMP-GSH2404L.

Chapter 7: Explanation on network technical terms from A to Z. Highly recommended for reference when you encounter an unfamiliar term.

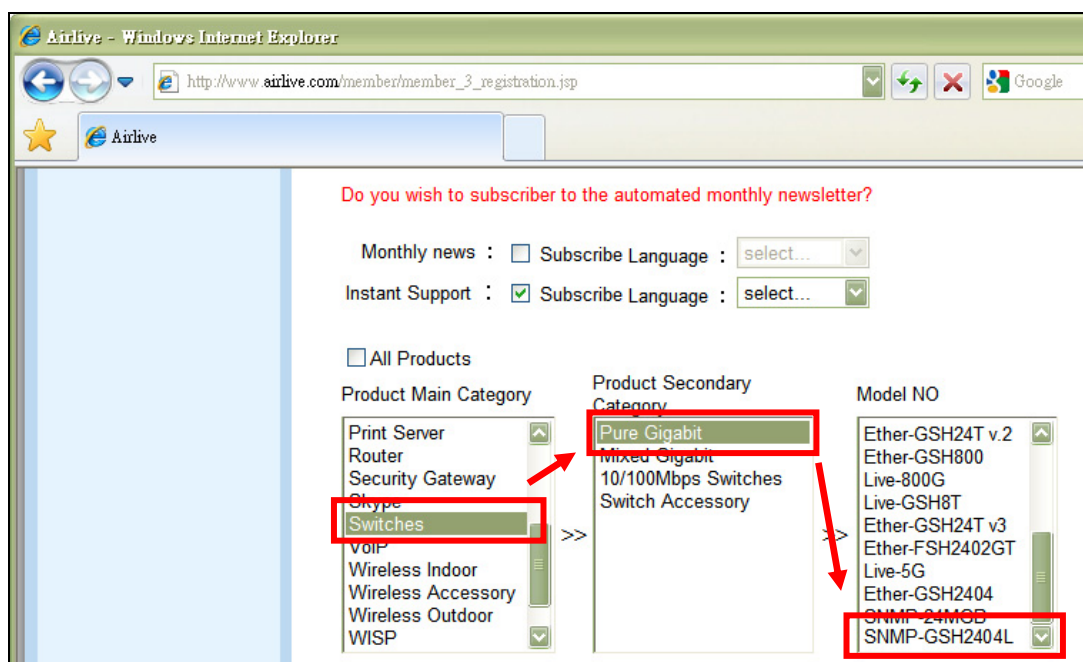
1.3 Firmware Upgrade and Tech Support

If you encounter a technical issue that can not be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmwares that either increase software functions or provide bug fixes for SNMP-GSH2404L. You can reach our on-line support center at the following link:

http://www.airlive.com/support/support_2.jsp

Since 2009, AirLive has added the “Newsletter Instant Support System” on our website. AirLive Newsletter subscribers receives instant email notifications when there are new download or tech support FAQ updates for their subscribed airlive models. To become an AirLive newsletter member, please visit: http://www.airlive.com/member/member_3.jsp



1.4 Features

- Confirms to IEEE802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit fiber
- 20 x 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports and 4x 10/100/1000Mbps TP or 1000Mbps SFP Fiber dual media auto sense
- High back-plane bandwidth 48Gbps
- 8K MAC address and support VLAN ID (1~4094)
- Power Saving with "ActiPHY Power Management" and "PerfectReach Power Management" techniques.
- Supports concisely the status of port and easily port configuration
- Supports per port traffic monitoring counters
- Supports a snapshot of the system Information when you login
- Supports port mirror function static trunk function
- Supports 802.1Q VLAN
- Supports user management and limits three users to login
- Maximal packet length can be up to 9600 bytes for jumbo frame application
- Supports Broadcasting Suppression to avoid network suspended or crashed
- Supports to send the trap event while monitored events happened
- Supports default configuration which can be restored to overwrite the current configuration which is working on via Web UI and Reset button of the switch
- Supports on-line plug/unplug SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 3
- Built-in web-based management to provide a more convenient GUI for the user
- Supports port mirror function with ingress/egress traffic
- Supports rapid spanning tree (802.1w RSTP)
- Supports 802.1X User Authentication
- Supports Ingress, Non-unicast and Egress Bandwidth rating management
- The trap event and alarm message can be transferred via e-mail
- Supports diagnostics to let administrator knowing the hardware status
- HTTP and TFTP for firmware upgrade, system log upload and configuration file import/export
- Supports remote boot the device through user interface and SNMP

2

Installing the SNMP-GSH2404L

This chapter describes the hardware features and the hardware installation procedure for the SNMP-GSH2404L. For software configuration, please go to chapter 3 for more details.

2.2 Before You Start

It is important to read through this section before you install the SNMP-GSH2404L.

- The maximum cabling distance is 100 meters.
- Do not create a network loop.
- Always check the LED lights for troubleshooting

2.3 Package Content

Unpack the contents of the SNMP-GSH2404L and verify them against the checklist below.

- One unit of SNMP-GSH2404L
- Power Cord
- Four Rubber Feet
- RS-232 cable
- User Guide (CD-ROM)
- Quick Installation Guide
- Rack-mounted Kit



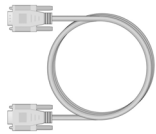
SNMP-GSH2404L



Power Cord



Four Rubber Feet



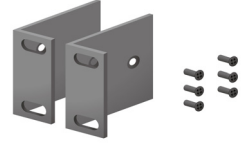
RS-232 cable



User Guide (CD-ROM)



Quick Installation Guide



Rack-mounted Kit

Compare the contents of your SNMP-GSH2404L package with the standard checklist above. If any item is missing or damaged, please contact your local dealer for service.

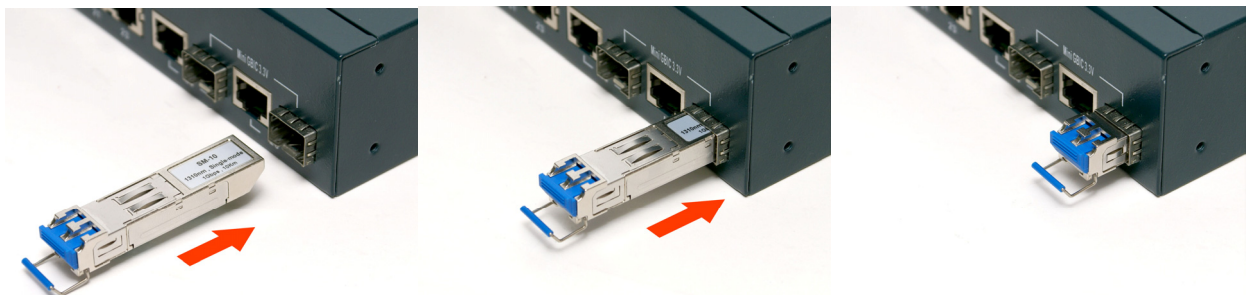
2.4 Optional Accessories

The SNMP-GSH2404L has the following optional accessories which you can purchase from AirLive

- 1000Base-SX MiniGBIC Transceiver (*Model: SFP-SX*) or 1000Base-LX MiniGBIC Transceiver (*Model: SFP-LX-10*) is for your SFP slots of SNMP-GSH2404L, it allows you to use fiber cable for extending transmission distance.

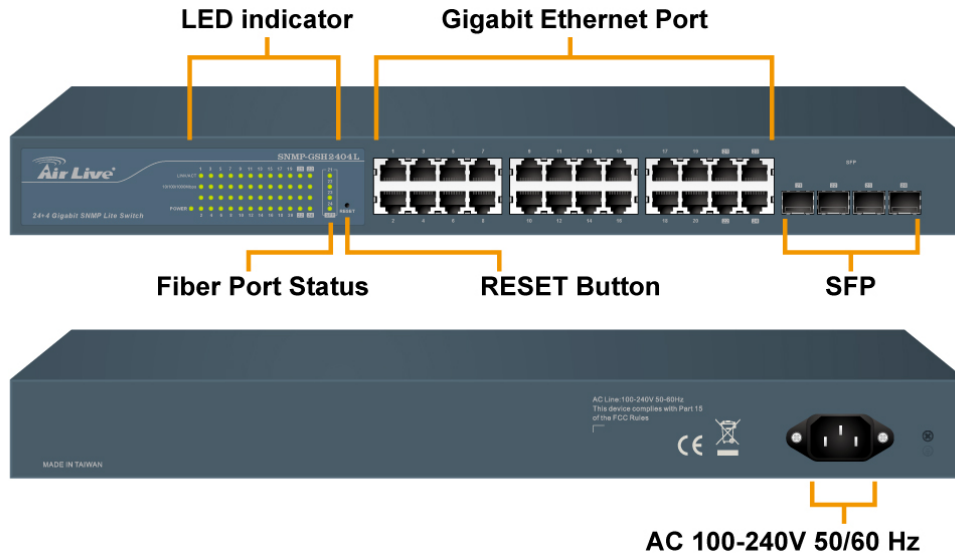


Note: While installing MiniGBIC into SFP slot of SNMP-GSH2404L, please notice the direction of MiniGBIC is correct, and make sure that MiniGBIC is indeed installed in the SNMP-GSH2404L.



2.5 Knowing your SNMP-GSH2404L

Below are descriptions and diagrams of the product:

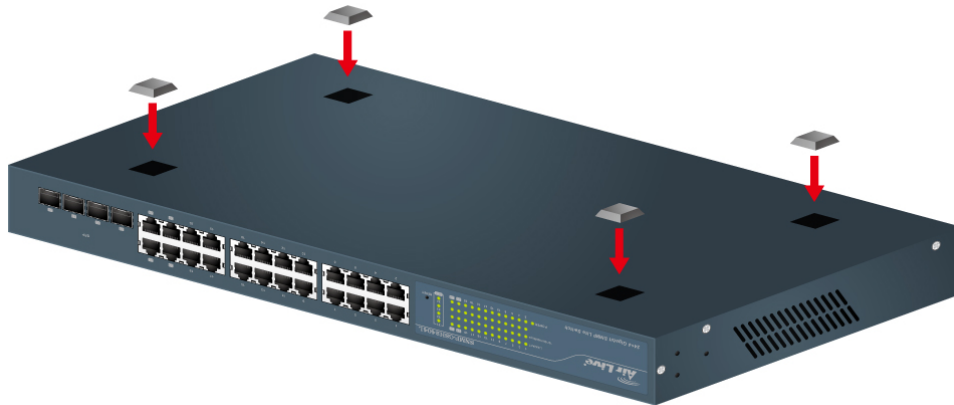


2.6 Hardware Installation

Set the SNMP-GSH2404L on a sufficiently large flat space with a power outlet nearby. The surface where you put your SNMP-GSH2404L should be clean, smooth, level and sturdy. Make sure there is enough clearance around the SNMP-GSH2404L to allow attachment of cables, power cord and allow air circulation.

2.6.1 Attaching Rubber Feet

- Make sure mounting surface on the bottom of the SNMP-GSH2404L is grease and dust free.
- Remove adhesive backing from your Rubber Feet.
- Apply the Rubber Feet to each corner on the bottom of the SNMP-GSH2404L. These footpads can prevent the Switch from shock/vibration.



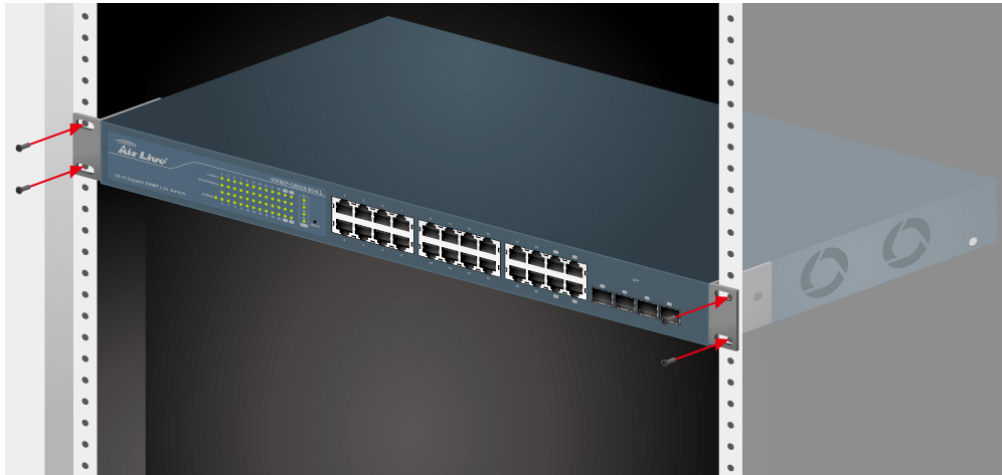
2.6.2 Rack-mounted Installation

The SNMP-GSH2404L comes with a rack-mounted kit and can be mounted in an EIA standard size, 19-inch Rack. The SNMP-GSH2404L can be placed in a wiring closet with other equipment. Perform the following steps to rack mount the SNMP-GSH2404L:

- A. Position one bracket to align with the holes on one side of the SNMP-GSH2404L and secure it with the smaller bracket screws. Then attach the remaining bracket to the other side of the SNMP-GSH2404L.



- B. After attached mounting brackets, position the SNMP-GSH2404L in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the SNMP-GSH2404L to the rack with a screwdriver and the rack-mounting screws.



Note: For proper ventilation, allow about at least 4 inches (10 cm) of clearance on the front and 3.4 inches (8 cm) on the back of the Switch. This is especially important for enclosed rack installation.

2.6.3 Power On

Connect the power cord to the power socket on the rear panel of the SNMP-GSH2404L. The other side of power cord connects to the power outlet. The internal power supply of the SNMP-GSH2404L works with voltage range of AC in the 100-240VAC, frequency 50~60Hz. Check the power indicator on the front panel to see if power is properly supplied.

2.7 LED Table

The LED Indicators gives real-time information of systematic operation status. The following table provides descriptions of LED status and their meaning.



LED	Status	Description
Power	Green	Power On
	Off	Power is not connected
10/100/1000BASE-T Port 1 to 24		
LNK/ACT	Green	The port is connecting with the device.
	Blink	The port is receiving or transmitting data.
	Off	No device attached.
10/100/1000Mbps	Green	In 1000Mbps connection speed
	Orange	In 100Mbps connection speed
	Off	In 10Mbps connection speed or no link
Gigabit Fiber Port 21 to 24		
SFP(LINK/ACT)	Green	The port is connecting with the device.
	Blink	The port is receiving or transmitting data.
	Off	Module connection is not good

3

Configuring the SNMP-GSH2404L

You can configure SNMP-GSH2404L through web browser (http). In this chapter, we will explain SNMP-GSH2404L's Web-based management interfaces and how to get into it. Then, we will provide the introduction on Web Management and recommended initial settings. For detail explanations on Web Management functions, please go to Chapter 4.

3.1 Important Information

The following information will help you to get start quickly. However, we recommend you to read through the entire manual before you start. Please note the username and password are case sensitive.

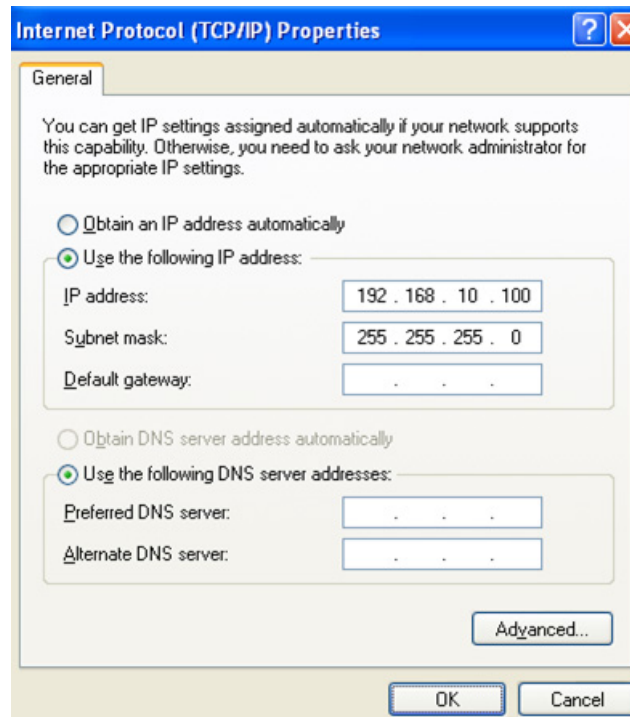
- ☐ The default IP address is **192.168.10.1**
- ☐ The default Subnet Mask is **255.255.255.0**
- ☐ The default Gateway is **192.168.1.254**
- ☐ The default username is **admin**
- ☐ The default password is **airlive**

3.2 Prepare your PC

The SNMP-GSH2404L can be managed remotely by a PC through RJ-45 cable. The default IP address of the SNMP-GSH2404L is **192.168.10.1** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the range of 192.168.1.2 to 192.168.1.253.

To prepare your PC for management with the SNMP-GSH2404L, please do the following:

1. Connect your PC directly to the copper port of SNMP-GSH2404L
2. Set your PC's IP address manually to 192.168.10.100 (or other address in the same subnet)



You are ready now to configure the SNMP-GSH2404L by using your PC.

3.3 Management Interface

The SNMP-GSH2404L can be configured using on the Web management interfaces.

- **Web Management (HTTP):** You can manage your SNMP-GSH2404L by simply typing its IP address in the web browser. Most functions of SNMP-GSH2404L can be accessed by web management inter face. We recommend using this interface for initial configurations. To begin, simply enter SNMP-GSH2404L's IP address (**default is 192.168.10.1**) on the web browser. The default username is **admin** and password is **airlive**.

3.4 Introduction to Web Management

The SNMP-GSH2404L offers Web Management interfaces for users. Users can easily access and control SNMP-GSH2404L via web browsers. The Web-Based Management supports Internet Explorer 5.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

3.4.1 Getting into Web Management

Web Management (HTTP)

1. Launch the Internet Explorer.
2. Type `http://192.168.1.1`. Press **“Enter”**.



3. The login screen appears.
4. Key in the user name and password. The default password is **“airlive”**.

Please enter password to login

Password:

Apply

5. Click **“Enter”** or **“Apply”**, then the home screen of the Web-based management appears.



Configuration
System Information
Ports
VLANs
--VLAN Mode
--VLAN Group
Aggregation
LACP
RSTP
802.1X
IGMP Snooping
Mirror
QoS
Filter
Rate Limit
Storm Control
SNMP
Monitoring
Detailed Statistics
LACP Status
RSTP Status
IGMP Status
Ping
Maintenance
Warm Restart
Factory Default
Software Upgrade
Configuration File Transfer
Logout



System Configuration

System Description	24+4 Gigabit SNMP Lite Switch
Firmware Version	V1.23
Hardware Version	v1.01
MAC Address	00-40-c7-3c-01-19
Serial Number	031802000028
Active IP Address	192.168.10.1
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.10.254
DHCP Server	0.0.0.0
Lease Time Left	0 secs

Device Name	SNMP-GSH2404L
System Contact	
System Location	
DHCP Enabled	<input type="checkbox"/>
Fallback IP Address	192.168.10.1
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	192.168.10.254
Management VLAN	1
Password	••••••••
Inactivity Timeout (0, 60-10000 Secs)	0

Apply

Refresh


4

Web Management in SNMP-GSH2404L

In this chapter, we will explain all settings in web management interface. Please be sure to read through Chapter 3's "Introduction to Web Management" first.

4.1 Menu Structure of SNMP-GSH2404L

The web management menu of SNMP-GSH2404L is divided into 3 parts: **Top Bar**, **Side Menu Bar**, and **Main Screen**.



Configuration

System Information

Ports

VLANs

--VLAN Mode

--VLAN Group

Aggregation

LACP

RSTP

802.1X

IGMP Snooping

Mirror

QoS

Filter

Rate Limit

Storm Control

SNMP

Monitoring

Detailed Statistics

LACP Status

RSTP Status

IGMP Status

Ping

Maintenance

Warm Restart

Factory Default


Software Upgrade

Configuration File Transfer

Logout

Side Menu

Top Bar



System Configuration

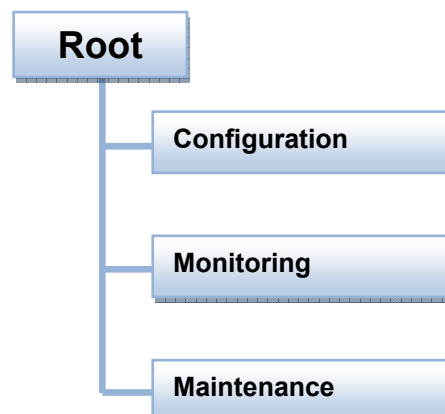
System Description	24+4 Gigabit SNMP Lite Switch
Firmware Version	V1.23
Hardware Version	v1.01
MAC Address	00-40-c7-3c-01-19
Serial Number	031802000028
Active IP Address	192.168.10.1
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.10.254
DHCP Server	0.0.0.0
Lease Time Left	0 secs

Device Name	SNMP-GSH2404L
System Contact	
System Location	
DHCP Enabled	<input type="checkbox"/>
Fallback IP Address	192.168.10.1
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	192.168.10.254
Management VLAN	1
Password	••••••
Inactivity Timeout (0, 60-10000 Secs)	0

Apply
Refresh

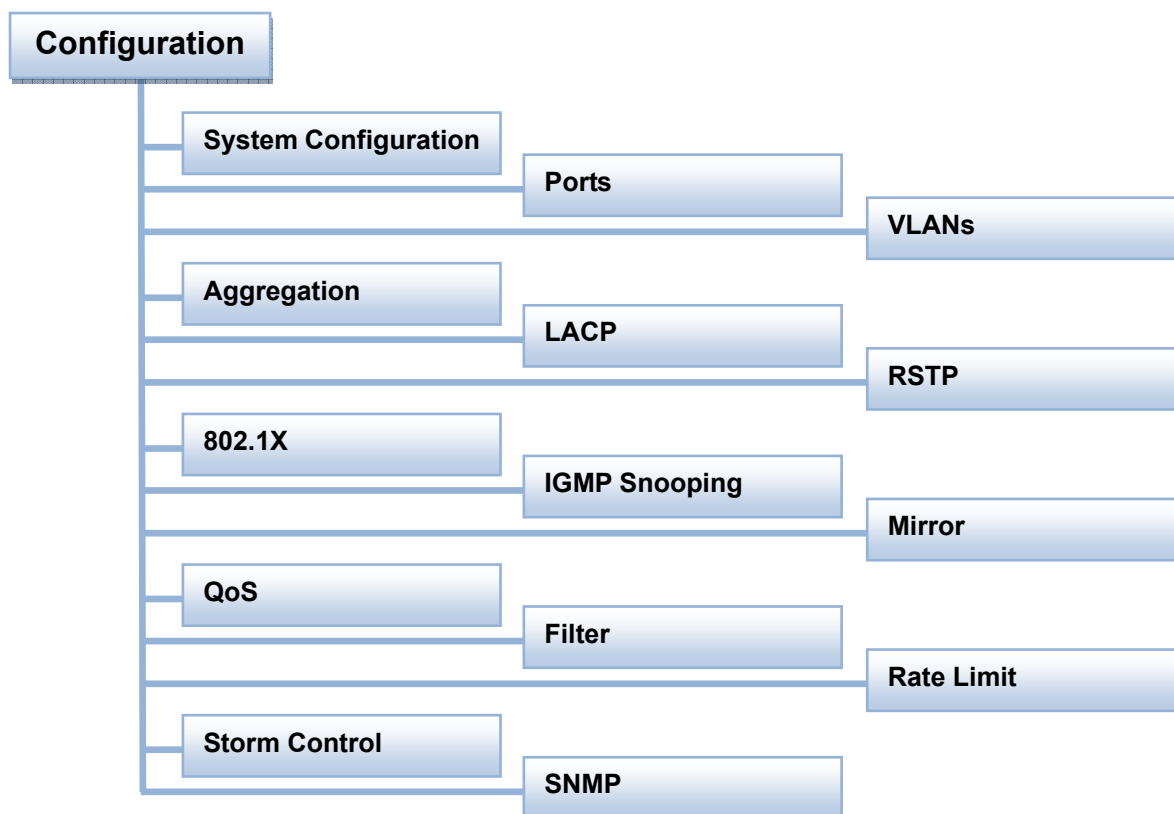
Main Screen

- **Top Bar:** It shows the front panel of the switch. Linked ports will be displayed in green color, and linked-off ones will be in black. For the optional modules, the slots with no module will only show covered plates, the other slots with installed modules would present modules. The images of modules would depend on the ones you insert. Vice versa, if ports are disconnected, they will show just in black.
- **Side Menu:** All management functions will show in Side Menu, you can choose any one of them to configure its setting. The detailed introduction for all management function will explain in below chapters. The following list is the full function tree for web user interface.
- **Main Screen:** Once choosing any function of Side Menu, the configuration page of the function will show in Main Screen. You can configure the function by instruction of manual. According to the function name in boldface, all functions can be divided into three parts, including “**Configuration**”, “**Monitoring**” and “**Maintenance**”. The functions of each folder are described in its corresponded section respectively. As to the function names in normal type are the sub-functions. When clicking it, the function is performed. The following list is the main function tree for web user interface.



4.2 Configuration

Configuration includes the following functions: System Configuration, Ports Configuration, VLAN Mode Configuration, VLAN Group Configuration, Aggregation, LACP, RSTP, 802.1X, IGMP Snooping, Mirror, QoS, Filter, Rate Limit, Storm Control and SNMP.



4.2.1 System Configuration

System configuration is one of the most important functions. Without a proper setting, network administrator would not be able to manage the device. The switch supports manual IP address setting.

System Configuration

System Description	24+4 Gigabit SNMP Lite Switch
Firmware Version	V1.23
Hardware Version	v1.01
MAC Address	00-40-c7-3c-01-19
Serial Number	031802000028
Active IP Address	192.168.10.1
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.10.254
DHCP Server	0.0.0.0
Lease Time Left	0 secs

Device Name	SNMP-GSH2404L
System Contact	
System Location	
DHCP Enabled	<input type="checkbox"/>
Fallback IP Address	192.168.10.1
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	192.168.10.254
Management VLAN	1
Password	••••••••
Inactivity Timeout (0, 60-10000 Secs)	0

[Apply](#)
[Refresh](#)

Function name:

System Configuration

Function description:

Show system description, firmware version, hardware version, MAC address, serial number, active IP address, active subnet mask, active gateway, DHCP server and Lease time left.

Set device name, DHCP enable, fallback IP address, fallback subnet mask, fallback gateway, management VLAN, password and inactivity timeout.

Parameter description:

System Description: The simple description of this switch.

Firmware Version:

The firmware version of this switch.

Hardware Version:

The hardware version of this switch.

MAC Address:

It is the Ethernet MAC address of the management agent in this switch.

Serial Number:

The serial number is assigned by the manufacturer.

Active IP Address:

Show the active IP address of this switch.

Active Subnet Mask:

Show the active subnet mask of this switch.

Active Gateway:

Show the active gateway of this switch.

DHCP Server:

Show the IP address of the DHCP server.

Default: 0.0.0.0

Lease Time Left:

Show the lease time left of DHCP client.

Device Name:

Set a special name for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character and null are acceptable.

Default: Giga Switch

DHCP Enabled:

Enable DHCP snooping, Just tick the check box (☒) to enable it.

Default: disable

Fallback IP Address:

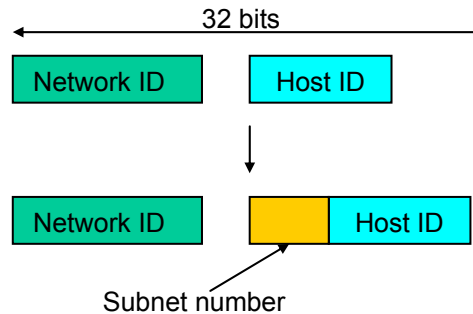
Users can configure the IP settings and fill in new values. Then, click **<Apply>** button to update.

Default: 192.168.1.1

Fallback Subnet Mask:

Subnet mask is made for the purpose to get more network address because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise can't communicate with other devices each other. But unfortunately, the network classes A, B, and C are all too large to fit for almost

all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total IP number of a network able to support, by the amount of 2 power of the bit number of subnet number ($2^{(\text{bit number of subnet number})}$).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

For more information, please also see the Section 2-1-4 “IP Address Assignment” in this manual.

Default: 255.255.255.0

Fallback Gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

Management VLAN:

Show the management VLAN number.

Password:

Set a password for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character is acceptable.

Default: admin

Inactivity Timeout(secs):

Set the auto-logout timer. The valid value is 0 ~ 60 in the unit of minute and a decimal point is not allowed. The value 0 means auto-logout timer is disabled.

Default: 0

4.2.2 Port

Function name:

Port Configuration

Function description:

Port Configuration is applied for the settings of the ports on the switch. By this function, you can set or reset the values for Mode and Flow Control. Others you could set the power saving mode for switch power consumption.

Port Configuration

Enable Jumbo Frames ☐
(Jumbo Frame support up to 9600 bytes.)

Perfect Reach/Power Saving Mode Disable

TP Ports

Port	Link	Mode	Flow Control	Flow Control Status
1	1000FDX	Auto Speed	<input type="checkbox"/>	disabled
2	Down	Auto Speed	<input type="checkbox"/>	disabled
3	Down	Auto Speed	<input type="checkbox"/>	disabled
4	Down	Auto Speed	<input type="checkbox"/>	disabled
5	Down	Auto Speed	<input type="checkbox"/>	disabled
6	Down	Auto Speed	<input type="checkbox"/>	disabled
7	Down	Auto Speed	<input type="checkbox"/>	disabled
8	Down	Auto Speed	<input type="checkbox"/>	disabled
9	Down	Auto Speed	<input type="checkbox"/>	disabled
10	Down	Auto Speed	<input type="checkbox"/>	disabled
11	Down	Auto Speed	<input type="checkbox"/>	disabled
12	Down	Auto Speed	<input type="checkbox"/>	disabled
13	Down	Auto Speed	<input type="checkbox"/>	disabled
14	Down	Auto Speed	<input type="checkbox"/>	disabled
15	Down	Auto Speed	<input type="checkbox"/>	disabled
16	Down	Auto Speed	<input type="checkbox"/>	disabled
17	Down	Auto Speed	<input type="checkbox"/>	disabled
18	Down	Auto Speed	<input type="checkbox"/>	disabled
19	Down	Auto Speed	<input type="checkbox"/>	disabled
20	Down	Auto Speed	<input type="checkbox"/>	disabled
21	Down	Auto Speed	<input type="checkbox"/>	disabled
22	Down	Auto Speed	<input type="checkbox"/>	disabled
23	Down	Auto Speed	<input type="checkbox"/>	disabled
24	Down	Auto Speed	<input type="checkbox"/>	disabled

Fiber Ports

Port	Link	Mode	Flow Control	Flow Control Status
21	Down	Auto Speed	<input type="checkbox"/>	disabled
22	Down	Auto Speed	<input type="checkbox"/>	disabled
23	Down	Auto Speed	<input type="checkbox"/>	disabled
24	Down	Auto Speed	<input type="checkbox"/>	disabled

Drop frames after excessive collisions ☐
(Use in Half Duplex flow control environment.)

Parameter description:

Enable Jumbo Frames:

This function support jumbo frames of up to 9600 bytes, Just tick the check box (☒) to enable it.

Default: disable

Perfect Reach/Power Saving Mode:

This function supports Power Saving and perfect Reach, Just select with the Full/ Link-up/ Link-down/ Disable

Default: disable

Link:

Show link status of this port.

Mode:

Set the speed and duplex of the port. If the media is 1Gbps fiber, there are three modes to choose: Auto Speed, 1000 Full and Disable. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

Media type	NWay	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto Speed mode, no default value. In Forced mode, default value depends on your setting.

Flow Control:

You can Just tick the check box (☒) to enable flow control. If flow control is set Enable, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Disable, there will be no flow control in the port. It drops the packet if too much to handle.

Default: Disable

Flow Control status:

To display the Flow control status.

4.2.3 VLAN Mode Configuration

The switch supports Port-based VLAN and Tag-based VLAN (802.1q). Its VLAN mode supports 24 active VLANs and the available VLAN ID range is from 1~4094. VLAN configuration is used to divide a LAN into smaller ones. With proper configuration, you can

gain not only improved security and increased performance, but also save a lot of VLAN management effort.

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes four modes: Port-based, Tag-based, Metro mode or Disable, you can choose one of them by pulling down list and pressing the <Downward> arrow key. Then, click <Apply> button, the settings will take affect immediately.

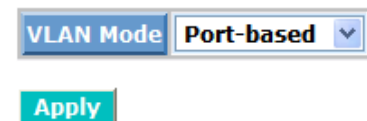
Parameter description:

VLAN Mode:

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximal 24 port-based VLAN groups.

VLAN Mode




The interface shows a dropdown menu labeled 'VLAN Mode' with 'Port-based' selected. Below it is a green 'Apply' button.

Tag-based:

Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q.

VLAN Mode



The interface shows a dropdown menu labeled 'VLAN Mode' with 'Tag-based' selected. Below it, there is a 'Double Tag' section with radio buttons for 'Disable' (selected) and 'Enable'. A green 'Apply' button is at the bottom.

Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 24 Tag VLAN groups.

Double-tag:

Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones

Metro Mode:

The Metro Mode is a quick configuration VLAN environment method on Port-based VLAN. It will create 21, 22, 23 or 24 Port-based VLAN groups.

VLAN Mode

VLAN Mode	Metro mode ▼
Up-link Port	21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 <input type="checkbox"/>
Apply	

Function name:

VLAN Port Configuration (Tag based VLAN mode)

Function description:

In VLAN Tag Rule Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rules to each port. There are two ingress filtering rules which can be applied to the switch. The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”. The Ingress Filtering Rule 2 is “drop untagged frame”. You can also select the Role of each port as Access, Trunk, or Hybrid.

Tag-Based VLAN Configuration

Add a VLAN

VLAN ID	<input type="text"/>
---------	----------------------

Add

VLAN Configuration List

Port Config

	VID	Description	Member
<input checked="" type="radio"/>	1	Default	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

NOTE:

Before deleting a VLAN, please make sure the PVID of all ports is different from the VID being deleted.

Modify **Delete** **Refresh**

VLAN Per Port Configuration

Port	Ingress Filtering Enabled	Packet Type	Role	Untagged VID	Pvid
Port 1	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 2	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 3	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 4	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 5	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 6	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 7	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 8	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 9	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 10	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 11	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼
Port 12	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	Access ▼	4094	1 ▼

Parameter description:

Port 1-24:

Port number.

Ingress Filtering Enabled:

Discard other VLAN group packets, only forward this port joined VLAN group packets.

Packet Type:

All: Forward all tagged and untagged packets.

Tagged Only: Forward tagged packets only and discard untagged packets.

Tag Out Enabled: It means the outgoing packets in this port must carry VLAN tag header.

Role:

This is an egress rule of the port. Here you can choose Access, Trunk or Hybrid. Trunk means the outgoing packets must carry VLAN tag header. Access means the outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. As to Hybrid, it is similar to Trunk, and both of them will tag-out. When the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packets with tag is the same as the one in the field of Untag VID of this port.

Untag VID:

Valid range is 1~4094. It works only when Role is set to Hybrid.

Pvid:

This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID.

4.2.4 VLAN Group Configuration

Function name:

VLAN Group Configuration

Function description:

It shows the information of VLAN Groups, and allows administrators to maintain them by modifying and deleting each VLAN group. User also can add a new VLAN group by inputting a new VLAN name and VLAN ID.

If you are in port-based VLAN, it will just show the ID、Member of the existed port-based VLAN group. If you are in tag-based VLAN, it will show the ID、VID、Member of the existed tag-based VLAN group. The switch can store the configuration of port-based VLAN and tag-based VLAN separately. When you choose one of VLAN mode, the switch will bring you the responded VLAN configuration which keeps the default data. You can easily create and delete a VLAN group by pressing **<Add>** and **<Delete>** function buttons, or click the Group ID directly to edit it.


Port-Based VLAN Configuration

Add a VLAN

ID	<input type="text" value="2"/>
----	--------------------------------

Add

VLAN Configuration List

	ID	Description	Member
	1	Default	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

Modify Delete Refresh

Parameter description:

ID (Group ID):

When you want to edit a VLAN group, you must select the Group ID field. Then, you will enter Tag Base VLAN Group Setting or Port Base VLAN Group Setting page, which depends on your VLAN mode selection.

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based mode.

Member:

In modify function this is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box (☒) beside the port x to enable it.

Add Group:

Create a new port-based VLAN or tag-based VLAN, which depends on the VLAN mode you choose in VLAN mode function.

VLAN Setup

Description			
ID: 2			
Port	Member	Port	Member
Port 1	<input type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

Delete Group:

Just tick the check box (☑) beside the ID, then press the **<Delete>** button to delete the group.

Port-Based VLAN Configuration

Add a VLAN

ID	3
----	---

Add

VLAN Configuration List

	ID	Description	Member
<input type="radio"/>	1	Default	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
<input checked="" type="radio"/>	2	dg	19,20

Modify Delete Refresh

4.2.5 Aggregation

The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle ports by same speed, MAC, and full duplex to be a single logical port, thus the logical port can aggregate the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if three Fast Ethernet ports are aggregated into a logical port, then this logical port's bandwidth would be as three times high as a single Fast Ethernet port's.

Function name:

Aggregation Configuration

Function description:

Display the current setup of Aggregation Trunking. With this function, user is allowed to add a new trunking group or modify the members of an existed trunking group.

Aggregation/Trunking Configuration

Group\Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Group 1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Group 2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Group 3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Group 4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Group 5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Group 6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Group 7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Group 8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Apply

Refresh

Parameter description:

Normal:

Set up the ports that do not join any aggregation trunking group.

Group 1~8:

Group the ports you choose together. Up to 12 ports can be selected for each group.

4.2.6 LACP

Smart Web Switch supports link aggregation IEEE802.3ad standard. The standard describes Link Aggregate Control Protocol (LACP) which dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention.

Function name:

LACP Port Configuration

Function description:

Enable or disable LACP protocol, user is allowed to set the aggregation key value.

LACP Port Configuration

Port	Protocol Enabled	Key Value (0~255)
1	<input type="checkbox"/>	auto
2	<input type="checkbox"/>	auto
3	<input type="checkbox"/>	auto
4	<input type="checkbox"/>	auto
5	<input type="checkbox"/>	auto
6	<input type="checkbox"/>	auto
7	<input type="checkbox"/>	auto
8	<input type="checkbox"/>	auto
9	<input type="checkbox"/>	auto
10	<input type="checkbox"/>	auto
11	<input type="checkbox"/>	auto
12	<input type="checkbox"/>	auto
13	<input type="checkbox"/>	auto
14	<input type="checkbox"/>	auto
15	<input type="checkbox"/>	auto
16	<input type="checkbox"/>	auto
17	<input type="checkbox"/>	auto
18	<input type="checkbox"/>	auto
19	<input type="checkbox"/>	auto
20	<input type="checkbox"/>	auto
21	<input type="checkbox"/>	auto
22	<input type="checkbox"/>	auto
23	<input type="checkbox"/>	auto
24	<input type="checkbox"/>	auto

Apply **Refresh**

Parameter description:

Protocol Enabled:

Just tick the check box (☒) to enable LACP protocol then press the **<Apply>** button to apply.

Key Value:

It's key for an aggregation. This must be an integer value between 1 and 255 or auto select by switch.

4.2.7 RSTP

In switches, bridges and routers. The protocol allows a switch to communicate with other RSTP compliant switches, and to ensure only one path existing between two stations in your network environment.

The switch allows you to create multiple STP configurations and assign ports to a specific tree.

Function name:

RSTP System Configuration

Function description:

This screen is used to display the RSTP system configuration and set the need of parameters.

Parameter description:

System Priority:

System priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box.

The lower the numeric value you assign, the higher the priority for this system.

Default: 32768

Hello Time:

This is the time interval in seconds between BPDU configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Default: 2

Max Age:

This is the maximum time a switch can wait without receiving a BPDU before attempting to reconfigure. The allowed range is 6 to 40 seconds.

Default: 20

Forward Delay:

This is the maximum time (in seconds) a switch will wait before changing states. The general rule: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$

Default: 15

Force version:

Select RSTP or STP protocol from the drop-down list box.

Function name:

RSTP Port Configuration

Function description:

Enable or disable RSTP protocol on the ports that are selected and set path cost.

Parameter description:

Protocol Enabled:

Just tick the check box (☒) beside the port x to enable RSTP protocol, then press the **<Apply>** button to apply.

Edge:

Just tick the check box (☒) beside the port x to enable edge function.

Path Cost:

Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost, user can select auto or set the rage from 1 to 200000000.

RSTP System Configuration

System Priority	32768
Hello Time	2
Max Age	20
Forward Delay	15
Force version	RSTP

RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost (1~200000000)
Aggregations	<input type="checkbox"/>		
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto

4.2.8 802.1X

802.1x port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through a 802.1x-enabled port without authentication. If a user wishes to touch the network through a port under 802.1x control, he (she) must firstly input his (her) account name for authentication and waits for gaining authorization before sending or receiving any packets from a 802.1x-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1x control, the devices or end stations connected to a controlled port send the authentication request to the authenticator, the authenticator pass the request to the authentication server to authenticate and verify, and the server tell the authenticator if the request get the grant of authorization for the ports.

According to IEEE802.1x, there are three components implemented. They are Authenticator, Supplicant and Authentication server shown in below figure.

Supplicant:

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE request to it.

Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

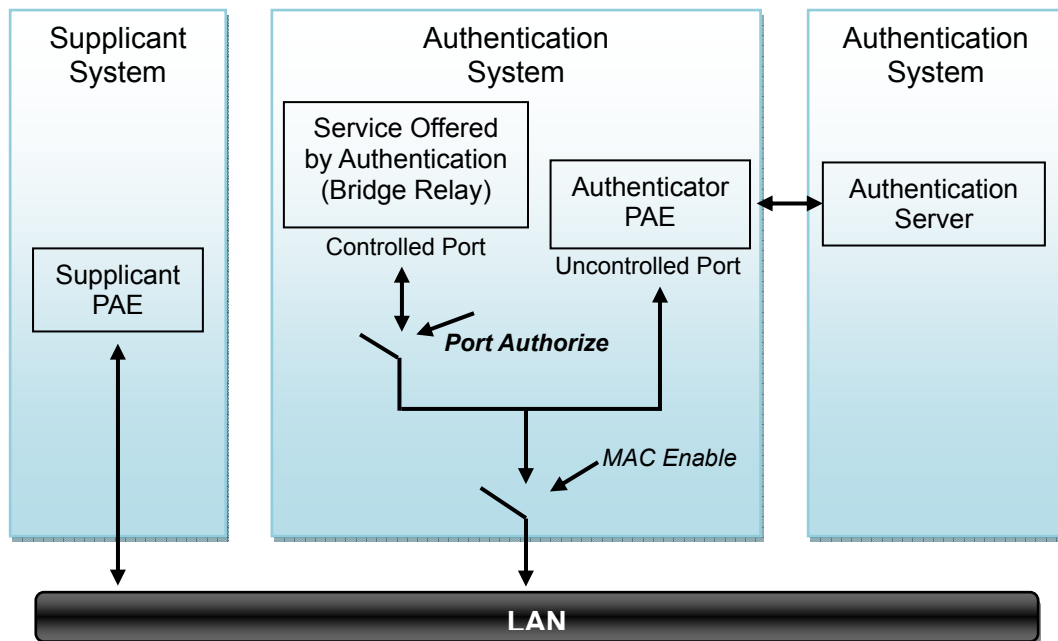
A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

Authentication server:

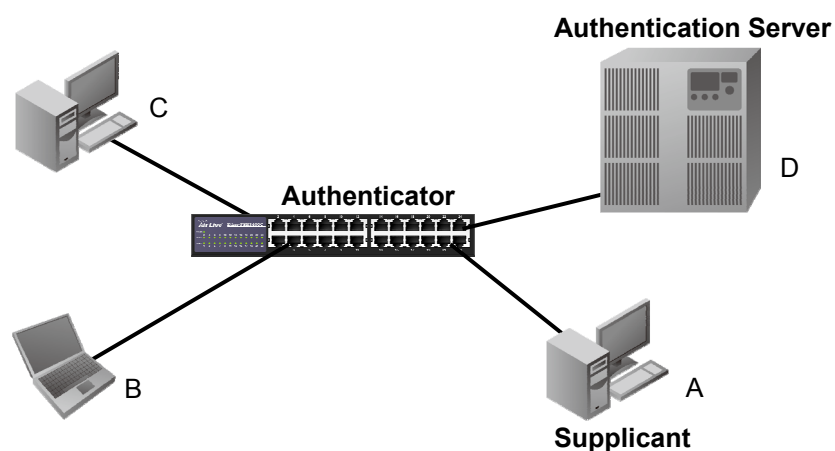
A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only touch the authenticator to perform authentication message exchange or access the network from the uncontrolled port.



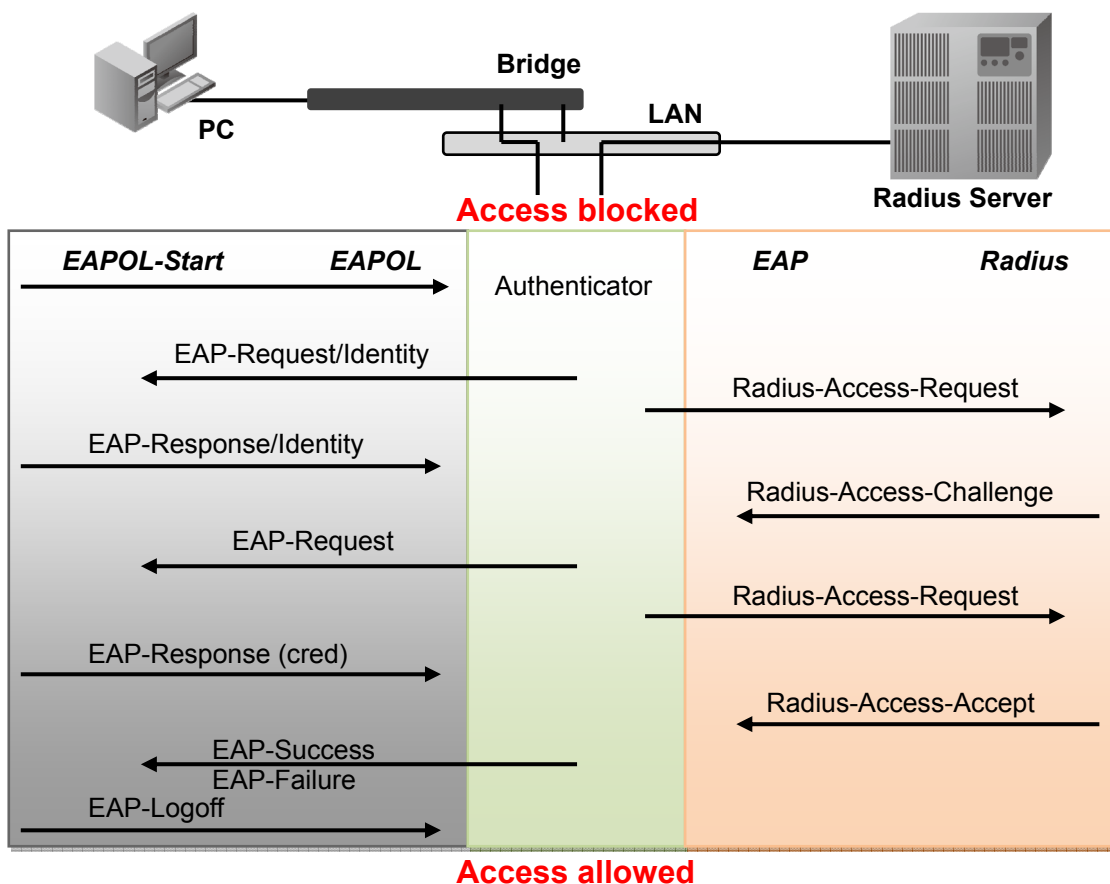
In the below figure, this is the typical configuration, a single supplicant, an authenticator and an authentication server. B and C is in the internal network, D is Authentication server running RADIUS, switch at the central location acts Authenticator connecting to PC A and A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C, first, it must exchange the authentication message with the authenticator on the port it connected via EAPOL packet. The authenticator transfers the supplicant's credentials to Authentication server for verification. If success, the authentication server will notice the authenticator the grant. PC A, then, is allowed to access B and C via the switch. If there are two switches directly connected together instead of single one, for the link connecting two switches, it may have to act two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.



The below figure shows the procedure of 802.1x authentication. There are steps for the

login based on 802.1x port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.
2. Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.
3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.
4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-Start the process by sending to the authenticator.
5. And next, the Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for confirming its identity.
6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant for asking for inputting user password via the authenticator PAE.
7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or other else algorithm.
8. If user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.
9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port connected to the supplicant and under 802.1x control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant is failed to authenticate. The port it connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.
10. When the supplicant issue an EAP-Logoff message to Authentication server, the port you are using is set to be unauthorized.



The 802.1X “Enabled” is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

802.1x Port-based Network Access Control function supported by the switch is little bit complex, for it just support basic “Enabled” mode, which can distinguish the device’s MAC address and its VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode, set in 802.1x Port mode, port control state, set in 802.1x port setting. Here Entry Authorized means MAC entry is authorized.

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Enabled	Auto	Successful	Port Authorized
Enabled	Auto	Failure	Port Unauthorized
Enabled	ForceUnauthorized	Don't Care	Port Unauthorized
Enabled	ForceAuthorized	Don't Care	Port Authorized

Function name:

802.1X Configuration

Function description:

This function is used to configure the global parameters for RADIUS authentication in 802.1x port security application.

Parameter description:

Mode:

Enable or disable 802.1X function.

RADIUS IP:

RADIUS server IP address for authentication.

Default: 0.0.0.0

RADIUS UDP Port:

The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535.

Default port number is 1812.

RADIUS Secret:

The secret key between authentication server and authenticator. It is a string with the length 1 – 15 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters.

Default: None

Admin State:

This is used to set the operation mode of authorization. There are three type of operation mode supported, Force Unauthorized, Force Authorized, Auto.

- Force Unauthorized: The controlled port is forced to hold in the unauthorized state.
- Force Authorized: The controlled port is forced to hold in the authorized state.
- Auto: The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

Default: Force Authorized

Port State:

Show the port status of authorization.

Re-authenticate:

Specify if subscriber has to periodically re-enter his or her username and password to stay connected to the port.

Re-authenticate All:

Re-authenticate for all ports in at once.

Force Reinitialize:

Force the subscriber has to reinitialize connected to the port.

Force Reinitialize All:

Force Reinitialize for all ports in at once.

802.1X Configuration

Mode:	Enabled ▾
RADIUS IP	0.0.0.0
RADIUS UDP Port	1812
RADIUS Secret	

Port	Admin State	Port State			
1	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
2	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
3	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
4	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
5	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
6	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
7	Force Authorized ▾	Authorized	Re-authenticate	Force Reinitialize	Statistics
8	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
9	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
10	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
11	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics
12	Force Authorized ▾	Link Down	Re-authenticate	Force Reinitialize	Statistics

Statistics:

Choose the port which you want to show of 802.1X statistics, the screen include Authenticator counters, backend Authenticator counters, dot1x MIB counters and Other statistics.

Press the **<Refresh>** button will fresh the screen and see the newer counters.

802.1X Statistics for Port 1

Refresh		Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
		Port 9	Port 10	Port 11	Port 12	Port 13	Port 14	Port 15	Port 16
		Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24
Authenticator counters									
authEntersConnecting	5					authEapLogoffsWhileConnecting			0
authEntersAuthenticating	0					authAuthSuccessesWhileAuthenticating			0
authAuthTimeoutsWhileAuthenticating	3					authAuthFailWhileAuthenticating			0
authAuthEapStartsWhileAuthenticating	0					authAuthEapLogoffWhileAuthenticating			0
authAuthReauthsWhileAuthenticated	0					authAuthEapStartsWhileAuthenticated			0
authAuthEapLogoffWhileAuthenticated	0								
Backend Authenticator counters									
backendResponses	0					backendAccessChallenges			0
backendOtherRequestsToSupplicant	4					backendAuthSuccesses			0
backendAuthFails	0								
dot1x MIB counters									
dot1xAuthEapolFramesRx	0					dot1xAuthEapolFramesTx			7
dot1xAuthEapolStartFramesRx	0					dot1xAuthEapolLogoffFramesRx			0
dot1xAuthEapolRespIdFramesRx	0					dot1xAuthEapolRespFramesRx			0
dot1xAuthEapolReqIdFramesTx	4					dot1xAuthEapolReqFramesTx			0
dot1xAuthInvalidEapolFramesRx	0					dot1xAuthEapolLengthErrorFramesRx			0
dot1xAuthLastEapolFrameVersion	0					dot1xAuthLastEapolFrameSource			
Other statistics									
Last Supplicant identity									

Function name:

802.1x Parameters

Function description:

In here, user can enable or disable Reauthentication function and specify how often a client has to re-enter his or her username and password to stay connected to the port.

Parameter description:

Reauthentication Enabled:

Choose whether regular authentication will take place in this port.

Default: disable

Reauthentication Period (1-65535 s):

A non-zero number seconds between the periodic re-authentication of the supplicant.

Default: 3600

EAP timeout ((1-255 s):

A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 –255.

Default: 30 seconds

802.1X Parameters

Reauthentication Enabled	<input type="checkbox"/> Enabled
Reauthentication Period [1-3600 seconds]	<input type="text" value="3600"/>
EAP timeout [1 - 255 seconds]	<input type="text" value="30"/>

4.2.9 IGMP Snooping

Function name:

IGMP Snooping Configuration

Function description:

IGMP Snooping lets administrators configure a switch to constrain multicast traffic by listening to Internet Group Management Protocol (IGMP). After finishing the settings, please press <**Apply**> button to start up the function.

Parameter description:

IGMP Enabled:

Just tick the check box (☒) to enable this function. Default: disable

Router Ports:

Just tick the check box (☒) beside the port x to enable router ports, then press the <Apply> button to start up. Default: none

Unregistered IGMP Flooding enabled:

Just tick the check box (☒) to enable this function. Default: enable

VLAN ID:

At the IGMP Enable mode being selected, it will list the VLAN ID number.

IGMP Snooping Enabled:

After IGMP Enabled function start up then user can tick the check box (☒) to enable this function. Default: enable

IGMP Querying Enabled:

After IGMP Enabled function start up then user can tick the check box (☒) to enable this function. Default: enable

IGMP Configuration

IGMP Enabled	<input type="checkbox"/>
Router Ports	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 <input type="checkbox"/>
Unregistered IPMC Flooding enabled	<input checked="" type="checkbox"/>

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
---	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

4.2.10 Mirror Configuration

Function name:

Mirror Configuration

Function description:

Mirror Configuration is provided to monitor the traffic in the network. This switch supports one-port mirror multi-ports. For example, we assume that Port A and Port B are Source Ports, and Port C is Mirror Port respectively, thus, the traffic passing through Port A and Port B will be copied to Port C for monitor purpose.

Parameter description:

Source Port:

Set up the port for being monitored. Just tick the check box (☒) beside the port x and valid port is Port 1~24.

Mirror Port:

Use the drop-down menu to select a mirror port.

Mirroring Configuration

Port	Mirror Source
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>
11	<input type="checkbox"/>
12	<input type="checkbox"/>
13	<input type="checkbox"/>
14	<input type="checkbox"/>
15	<input type="checkbox"/>
16	<input type="checkbox"/>
17	<input type="checkbox"/>
18	<input type="checkbox"/>
19	<input type="checkbox"/>
20	<input type="checkbox"/>
21	<input type="checkbox"/>
22	<input type="checkbox"/>
23	<input type="checkbox"/>
24	<input type="checkbox"/>

Mirror Port	1
-------------	---

Apply	Refresh
-------	---------

4.2.11 QoS Configuration

The switch offers powerful QoS function. This function supports VLAN-tagged priority that can make precedence of 8 priorities, and DSCP(Differentiated Services Code Point) on Layer 3 of network framework.

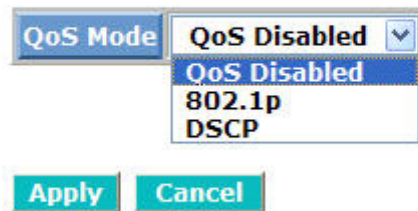
Function name:

QoS Configuration

Function description:

While setting QoS function, please select QoS Mode in drop-down menu at first. Then you can use 802.1p Priority and DSCP Priority functions. In this function, you can enable/disable QoS Mode and set Priority Control, such as: 802.1p and DSCP. The switch only supports Strict Priority. High priority queue is always passed first.

QoS Configuration



The dialog box titled "QoS Configuration" contains a label "QoS Mode" next to a dropdown menu. The dropdown menu is currently set to "QoS Disabled" and shows a list of options: "QoS Disabled", "802.1p", and "DSCP". Below the dropdown menu are two buttons: "Apply" and "Cancel".

Function name:

802.1p QoS Mode

Function description:

This function will affect the priority of VLAN tag. Based on priority of VLAN tag, it can arrange 0~7 priorities, priorities can map to 4 queues of the switch (low, normal, medium, high) and possess different bandwidth distribution according to your weight setting.

Parameter description:

Prioritize Traffic

Five Prioritize Traffic values are provided: Custom, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.

The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.

Port Number

When Custom is selected for Prioritize Traffic, you may assign specific Port Number for 802.1p Configuration.

802.1p Configuration:

Each Priority can select any of Queue. In Default, Priority 0 is mapping to Queue normal, Priority 1 is mapping to Queue low, Priority 2 is mapping to Queue low, Priority 3 is mapping to Queue normal, Priority 4 is mapping to Queue medium, Priority 5 is mapping to Queue medium, Priority 6 is mapping to Queue high, and Priority 0 is mapping to Queue high.

QoS Configuration

QoS Mode	802.1p
Prioritise Traffic	Custom
Port Number	Port 1

802.1p Configuration							
802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	low	1	low	2	normal	3	normal
4	medium	5	medium	6	high	7	high

Function name:

DSCP QoS Mode

Function description:

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

DSCP can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to any of queue (low, normal, medium, high).

Parameter description:

Prioritize Traffic

Five Prioritize Traffic values are provided: Custom, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.

The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.

Port Number

When Custom is selected for Prioritize Traffic, you may assign specific Port Number for DSCP Configuration.

DSCP Configuration:

64 kinds of priority traffic as mentioned above, user can set up any of Queue (low, normal, medium, high). In default, Priority 0~63 are mapping to Queue high.

QoS Configuration

QoS Mode	DSCP
Prioritise Traffic	All High Priority
Port Number	Port 1

DSCP Configuration	
DSCP Value(0..63)	Priority
	high
	high
	high
	high
	high
	high
	high
All others	high

Apply	Cancel
-------	--------

4.2.12 Filter

Function name:

Filter Configuration

Function description:

This function lets administrators easily set management source IP addresses to the ports on the switch. After completing the settings, please press **<Apply>** button to make this function take effect.

Filter Configuration

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled			<input checked="" type="checkbox"/>
2	Disabled			<input checked="" type="checkbox"/>
3	Disabled			<input checked="" type="checkbox"/>
4	Disabled			<input checked="" type="checkbox"/>
5	Disabled			<input checked="" type="checkbox"/>
6	Disabled			<input checked="" type="checkbox"/>
7	Disabled			<input checked="" type="checkbox"/>
8	Disabled			<input checked="" type="checkbox"/>
9	Disabled			<input checked="" type="checkbox"/>
10	Disabled			<input checked="" type="checkbox"/>
11	Disabled			<input checked="" type="checkbox"/>
12	Disabled			<input checked="" type="checkbox"/>
13	Disabled			<input checked="" type="checkbox"/>

Parameter description:

Source IP Filter:

Mode:

There are three types of mode in this drop-down menu. Default is disabled.

Disabled:

Allow all IP Address login to this switch and manage it.

Static:

Just allow the IP Address which set by administrator to login to this switch and manage it..

DHCP:

Allow the IP Address get from DHCP server can login to this switch and manage it.

Note: If you choose this mode only an DHCP client could be packet forwarding on the port.

IP Address:

Setting up the IP Address, it can be one IP Address or a LAN.

IP Mask:

Setting up the IP Subnet Mask related with the IP Address.

DHCP Server Allowed:

Just tick the check box (☒) under the port x to allow the DHCP Server on this port and valid port is Port 1~24. Default: enable.

Parameter description:

Ingress:

Set up the limit of Ingress bandwidth (Range: 128Kb, 512Kb, 1M, 10M and 32M) for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges is from Rate1 to 29.

Default: No Limit

Egress:

Set up the limit of Egress bandwidth (Range: 128Kb, 512Kb, 1M, 10M and 32M) for the port you choose. Outgoing traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges is from Rate1 to 29. Default: No Limit.

4.2.14 Storm Control

Function name:

Storm Control

Function description:

Storm Control is used to block unnecessary multicast and broadcast frames that reduce switch's performance. When the function is enabled and Storm Control rate settings are detected as exceeded, the unnecessary frames would be dropped.

Storm Control Configuration

Storm Control Number of frames per second	
ICMP Rate	No Limit
Learn Frames Rate	1k
Broadcast Rate	2k
Multicast Rate	4k
Flooded unicast Rate	8k
	16k
	32k
	64k
	128k
	256k
	512k
	1024k
	No Limit

Parameter description:**ICMP Rate:**

To enable the ICMP Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

Learn Frames Rate:

To enable the Learn Frames Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

Broadcast Rate:

To enable the Broadcast Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

Multicast Rate:

To enable the Multicast Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

Flooded unicast Rate:

To enable the Flooded unicast Storm capability. User can use drop-down menu to select number of frames. Default is No Limit. The setting range is 1k~1024k per second.

NOTE: After completing the function's setting, press **<Apply>** button to have this function taken effect.

4.2.15 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. It is a protocol used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will be started up. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Function name:

SNMP Configuration

Function description:

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click **<Apply>** button, the setting takes effect.

SNMP Configuration

SNMP enabled	<input checked="" type="checkbox"/>
SNMP Trap destination	0.0.0.0
SNMP Get Community	public
SNMP Set Community	private
SNMP Trap Community	public

System Event	<input checked="" type="checkbox"/> Cold Boot	<input checked="" type="checkbox"/> Warm Boot
TP and Fiber Port Event	<input checked="" type="checkbox"/> Link Up	Link Up Counter 1
	<input checked="" type="checkbox"/> Link Down	Link Down Counter 0

Apply	Refresh
-------	---------

Parameters description:

SNMP enable:

The term SNMP enable here is used for the activation or de-activation of SNMP. Default is "Disable".

Get/Set/Trap Community:

Community name is used as password for authenticating if the requesting network management unit belongs to the same community group. If they both don't have the same community name, they don't belong to the same group. Hence, the requesting network management unit can not access the device with different community name via SNMP protocol; If they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. There is not allowed to put any blank in the community name string. Any printable character is allowable.

The community name for each function works independently. Each function has its own community name. Say, the community name for Read only works for Read function and can't be applied to other function such as Write and Trap.

Default SNMP function: Disable

Default community name for Get: public

Default community name for Set: private

Default community name for Trap: public

System Event:

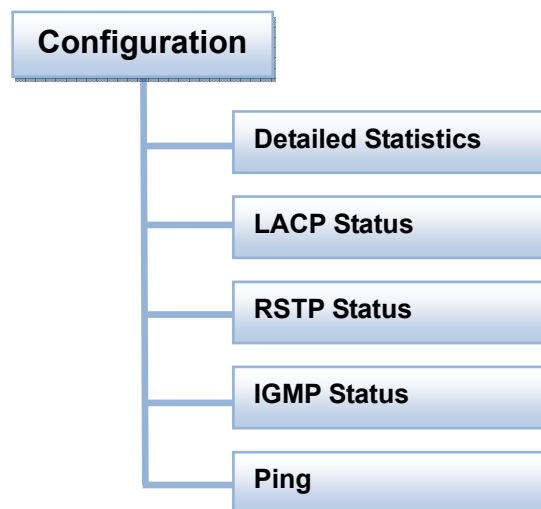
The System Event trap enable here is used for the “Cold Boot” or “Warm Boot” of system Event. Default is “Disable”.

TP and Fiber Port Event:

The TP and Fiber Port Event trap enable here is used for the “Link Up” or “Link Down” of system Event. Default is “Disable”.

4.3 Monitor

There are five functions contained in the monitoring function.



4.3.1 Detailed Statistics

Function name:

Detailed Statistics

Function description:

Display the detailed counting number of each port's traffic. The window can show all counter information each port at one time.

Configuration System Information Ports VLANs --VLAN Mode --VLAN Group Aggregation LACP RSTP 802.1X IGMP Snooping Mirror QoS Filter Rate Limit Storm Control SNMP Monitoring Statistics Overview Detailed Statistics LACP Status RSTP Status IGMP Status Ping Maintenance Warm Restart Factory Default	Statistics for Port 1							
	Clear Refresh		Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
			Port 9	Port 10	Port 11	Port 12	Port 13	Port 14
			Port 17	Port 18	Port 19	Port 20	Port 21	Port 22
			Port 23	Port 24				
	Receive Total				Transmit Total			
	Rx Packets				Tx Packets			
	33215				21520			
	Rx Octets				Tx Octets			
	3390475				5121779			
	Rx High Priority Packets				Tx High Priority Packets			
	-				-			
	Rx Low Priority Packets				Tx Low Priority Packets			
	-				-			
	Rx Broadcast				Tx Broadcast			
	-				-			
	Rx Multicast				Tx Multicast			
	-				-			
	Rx Broad- and Multicast				Tx Broad- and Multicast			
	1021				0			
	Rx Error Packets				Tx Error Packets			
	0				0			
Receive Size Counters				Transmit Size Counters				
Rx 64 Bytes				Tx 64 Bytes				-
-				-				-
Rx 65-127 Bytes				Tx 65-127 Bytes				-
-				-				-
Rx 128-255 Bytes				Tx 128-255 Bytes				-
-				-				-
Rx 256-511 Bytes				Tx 256-511 Bytes				-
-				-				-
Rx 512-1023 Bytes				Tx 512-1023 Bytes				-
-				-				-
Rx 1024- Bytes				Tx 1024- Bytes				-
-				-				-
Receive Error Counters				Transmit Error Counters				
Rx CRC/Alignment				Tx Collisions				-
-				-				-

Parameter description:

Rx Packets:

The counting number of the packet received.

RX Octets:

Total received bytes.

Rx High Priority Packets:

Number of Rx packets classified as high priority.

Rx Low Priority Packets:

Number of Rx packets classified as low priority.

Rx Broadcast:

Show the counting number of the received broadcast packet.

Rx Multicast:

Show the counting number of the received multicast packet.

Rx Broad- and Multicast:

Show the counting number of the received broadcast with multicast packet.

Rx Error Packets:

Show the counting number of the received error packets.

Tx Packets:

The counting number of the packet transmitted.

TX Octets:

Total transmitted bytes.

Tx High Priority Packets:

Number of Tx packets classified as high priority.

Tx Low Priority Packets:

Number of Tx packets classified as low priority.

Tx Broadcast:

Show the counting number of the transmitted broadcast packet.

Tx Multicast:

Show the counting number of the transmitted multicast packet.

Tx Broad- and Multicast:

Show the counting number of the transmitted broadcast with multicast packet.

Tx Error Packets:

Show the counting number of the received error packets.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes:

Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment:

Number of Alignment errors and CRC error packets received.

Rx Undersize:

Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize:

Number of long frames(according to max_length register) with valid CRC.

Rx Fragments:

Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber:

Number of long frames(according to max_length register) with invalid CRC.

Rx Drops:

Frames dropped due to the lack of receiving buffer.

Tx Collisions:

Number of collisions transmitting frames experienced.

Tx Drops:

Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx Overflow:

Number of frames dropped due to the lack of transmitting buffer.

4.3.2 LACP Status

Function name:

LACP Status

Function description:

Display LACP status. It illustrates that LACP Status window can show LACP information and status for all ports in the same time.

- Configuration
- System Information
- Ports
- VLANs
 - VLAN Mode
 - VLAN Group
- Aggregation
- LACP
- RSTP
- 802.1X
- IGMP Snooping
- Mirror
- QoS
- Filter
- Rate Limit
- Storm Control
- SNMP
- Monitoring
- Statistics Overview
- Detailed Statistics
- LACP Status
- RSTP Status
- IGMP Status
- Ping
- Maintenance
- Warm Restart
- Factory Default

LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Normal																							

Legend

Down	Port link down
0 Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0 Learning	Port Learning by RSTP
Forwarding	Port link up and forwarding frames
0 Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

LACP Port Status

Parameter description:

LACP Aggregation Overview:

Show the group/port status. Default will set to red sign for port link down, user can check legend table below for all reference.

LACP Port Status:

Group/Port:

Show the port number.

Normal : as Legend.

4.3.3 RSTP Status

Function name:

RSTP Status

Function description:

Display RSTP status. The below figure shows you that RSTP window can present VLAN bridge information and the status of all ports.

RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-a0-57-15-2a-f2	2	20	15	Steady	This switch is Root!

[Refresh](#)

RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP
Port 9						Non-STP

Parameter description:

RSTP VLAN Bridge Overview:

VLAN Id:

Show the VLAN Id.

Bridge Id:

Show this switch's current bridge priority setting and bridge ID which stands for the MAC address of this switch.

Hello Time:

Show the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending hello message every "hello time" seconds to the bridge attached to its designated port.

Max Age:

Show the root bridge's current max age time.

Fwd Delay:

Show the root bridge's forward delay time.

Topology:

Show the root bridge's spanning tree topology.

Root Id:

Show root bridge ID of this network segment. If this switch is a root bridge, the "This switch is Root" will show this switch's bridge ID.

4.3.4 IGMP Status

Function name:

IGMP Status

Function description:

Display IGMP status. It shows VLAN ID for each multicast group.

IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Idle	0	0	0	0	0	0

IGMP Status

Page:1

VLAN ID	IP Address	Ports
1	No active groups	---

Refresh	First Page	Prev Page	Next Page
---------	------------	-----------	-----------

Parameter description:

VLAN Id:

Show VLAN Id for each multicast group.

Querier:

Show the group membership queries status.

Queries transmitted:

To count the group membership queries transmitted.

Queries received:

To count the group membership queries received.

V1 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the *Max Response Time* field in the query,

for each group to which it belongs. It Calculate the number of times of IGMPV1 report.

V2 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the *Max Response Time* field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV2 report.

V3 Reports:

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the *Max Response Time* field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV3 report.

V2 Leaves:

When a host leaves a group, it sends a leave group membership message to multicast routers on the network, it show the leaves number.

4.3.5 Ping Status

Function name:

Ping Status

Function description:

To set up target IP address for ping function and display ping status. It shows the ping information.

Ping Parameters

Target IP address	<input type="text"/>
Count	1 <input type="button" value="v"/>
Time Out (in secs)	1 <input type="button" value="v"/>

Apply

Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Parameter description:

Ping Parameters:

Target IP address:

Set up a Target IP address to ping.

Count:

Use drop-down menu to set number of echo requests to send. Four type of number can choose, there are 1, 5, 10 and 20.

Default: 1

Time Out (in secs):

Use drop-down menu to set number of echo requests time out in second. Four type numbers can choose, there are 1,5,10 and 20.

Default: 1

NOTE: All the functions should press **<Apply>** button to start up after you set up the parameters.

Ping Results:

Target IP address:

Show the active target IP address.

Status:

Show the result of the ping status.

Received replies:

Show the received replies number of times.

Request timeouts:

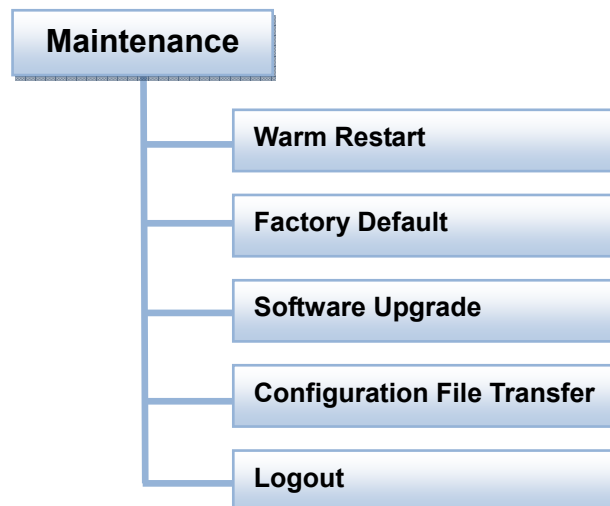
Show the timeout of request.

Average Response times (In ms):

Show the average response time in milliseconds.

4.4 Maintenance

There are five functions contained in the maintenance function.



4.4.1 Warm Restart

Web Smart Switch offers many approaches to reboot your switch, such as: power up, hardware reset and software reset. You can press RESET button in the front panel of your switch to reset the device and to retrieve default settings. After upgrading software, you have to reboot the device to have new configuration take effect. The function being discussed here is software reset.

Function name:

Warm Restart

Function description:

Reboot the switch. Reboot takes the same effect as the RESET button on the front

panel of the switch. Press **<Yes>** button to confirm warm restart function and it will take around thirty (30) seconds to complete the system boot.

Warm Restart



Are you sure you want to perform a Warm Restart?

4.4.2 Factory Default

Function name:

Factory Default

Function description:

Factory Default provides the function to retrieve default settings and replace current configuration. Except the IP address setting, all settings will be restored to the factory default values when “Factory Default” function is performed. If you want to restore all configurations including the IP address setting to the factory default, please press the “RESET” button on the front panel.

“RESET” button: You must press the “RESET” button in front panel over 3 seconds to restore the factory default setting.

Factory Default



Are you sure you want to perform a Factory Default?

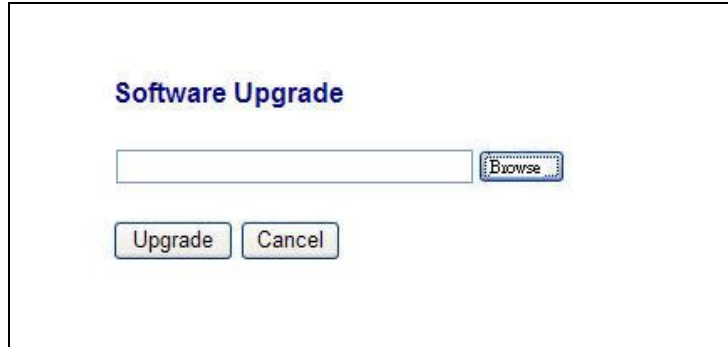
4.4.3 Software Upgrade

Function name:

Software Upgrade

Function description:

You can just click Browse button to retrieve the file you want in your system to upgrade your switch.



The image shows a web-based dialog box titled "Software Upgrade". It contains a text input field for a file path, followed by a "Browse" button. Below the input field are two buttons: "Upgrade" and "Cancel".

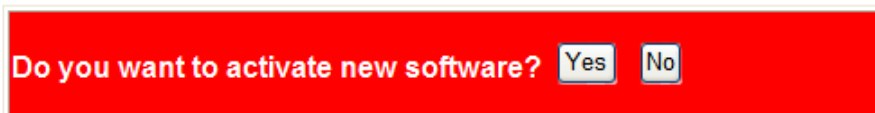
Once clicking "Upgrade" button, the windows will show upgrading progress as below figure

Software Upgrade Progress



After a while, window will tell user that "Software Successfully loaded" and will ask you if you want to activate new software.

Software successfully loaded



The image shows a red dialog box with the text "Do you want to activate new software?" in white. To the right of the text are two buttons: "Yes" and "No".

Then, the Switch will reboot automatically.

System Reboot will take a couple of seconds...

4.4.4 Configuration File Transfer

Function name:

Configuration File Transfer

Function description:

You can backup your switch's configuration file into your computer folder in case accident happens. In addition, uploading backup configuration file into a new or a crashed switch can save much time and avoid mistakes.

Configuration Upload

Configuration Download

4.4.5 Logout

In addition to auto logout function we just mentioned in system configuration section, the switch also allows administrators to logout manually by Logout function.

Function name:

Logout

Function description:

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can set up the parameter of Auto Logout Timer in system configuration function to explicitly ON/OFF this logout function.

Maintenance
Warm Restart
Factory Default
Software Upgrade
Configuration File Transfer
Logout

Parameter description:

Auto/Manual Logout:

If no action and no key is stroke as well in any function screen more than the minutes you set up in Auto Logout Timer, the switch will have you logout automatically. Or press the **<Logout>** button in Logout function to exit the system manually.

5

Troubleshooting

This section is intended to help you solve the most common problems on the SNMP-GSH2404L.

5.1 Incorrect connections

The switch port can auto detect straight or crossover cable when you link switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps port use 2 pairs twisted cable and Gigabit 1000T port use 4 pairs twisted cable. If the RJ-45 connector is not correct pin on right position then the link will fail. For fiber connection, please notice that fiber cable mode and fiber module should be match.

■ Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. IF that does not correct the problem, try a different cable.

■ Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5-cable tester is a recommended tool for every 100Base-T network installation.

■ Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

5.2 Diagnosing LED Indicators

The SNMP-GSH2404L can be easily monitored through panel indicators to assist in identifying problems, which describes common problems you may encounter and where you can find possible solutions. Please refer to Chapter 2.7 for detailed information.

If the power indicator does turn on when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the Switch powers off after running for a while check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact your local dealer for assistance.

5.3 Cabling

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections or 100Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5 or cat-5e cable for 1000Mbps connections. The length does not exceed 100 meters.

6

Specifications

This section provides the specifications of SNMP-GSH2404L, and the following table lists these specifications.

Standard	<ul style="list-style-type: none"> ● IEEE802.3 10BASE-T ● IEEE802.3u 100BASE-TX ● IEEE802.3z Gigabit SX/LX ● IEEE802.3ab Gigabit 1000TX ● IEEE802.3x Flow Control and Back pressure ● IEEE802.3ad Port trunk with LACP ● IEEE802.1d Spanning tree protocol ● IEEE802.1p Class of service ● IEEE802.1Q VLAN Tagging ● IEEE802.1X Access Control ● IEEE802.1d Spanning Tree ● IEEE802.1w Rapid Spanning Tree
Interface	<ul style="list-style-type: none"> ● 20 x 10/100/1000Mbps ● 4 x 10/100/1000Mbps/Mini-GBIC ports
Switch architecture	<ul style="list-style-type: none"> ● Store and forward switch architecture. ● Back-plane up to 48Gbps
Power Saving	<ul style="list-style-type: none"> ● Auto Detect client idle or cable length
Switching Capacity	<ul style="list-style-type: none"> ● 48Gbps forwarding bandwidth
MAC address	<ul style="list-style-type: none"> ● 8K
Jumbo Frame	<ul style="list-style-type: none"> ● 9600 bytes
Memory	<ul style="list-style-type: none"> ● 500 KB for packet buffer

LED	<ul style="list-style-type: none"> ● System power ● 10/100/1000M TP Port 1 to 24: LINK/ACT, 10/100/1000Mbps ● 1000M SFP Fiber Port 21 to 24: SFP(LINK/ACT)
Management	<ul style="list-style-type: none"> ● Web/ SNMP v1,v2c management ● RFC Standard <ul style="list-style-type: none"> ■ SNMP agent : MIB-II (RFC 1213) ■ Bridge MIB (RFC 1493) ■ Interface Group MIB (RFC 2863) ● SNMP Trap ● Firmware upgradeable ● Port Trunk <ul style="list-style-type: none"> ■ Support IEEE802.3ad with LACP function. ■ Up to 12 trunk groups and group member up to 12. ● Supports IEEE802.1d STP & IEEE802.1w RSTP ● VLAN <ul style="list-style-type: none"> ■ Port-based VLAN ■ IEEE 802.1Q Tag-based VLAN, 4094 max, up to 24 active VLANs including static and dynamic entry ■ Tag-based VLAN supports egress/ingress packet filter ● QoS policy: <ul style="list-style-type: none"> ■ Supports port-based, Tag-based, IPv4 ToS and DSCP ■ Supports 802.1p QoS with 4 level priority queue ■ Supports two scheduling, WRR and Strict ● Supports IGMP snooping ● Supports Port Mirroring ● Supports Unknown Unicast / Multicast / Broadcast Storm Control ● Supports ingress and egress per port bandwidth control with 1Mbps increment ● Supports 802.1x access control for port-based

	authentication
MTBF	<ul style="list-style-type: none"> ● 68655 (hr)
Temperature	<ul style="list-style-type: none"> ● Operating: 0 to 40°C ● Storage: -10 to 70°C
Humidity	<ul style="list-style-type: none"> ● Operating: 10% ~ 90% ● Storage: 5% ~ 90%
Power	<ul style="list-style-type: none"> ● 100~240VAC 50/60Hz (maximum) ● Power consumption 20Watts
Produce Weight (g)	<ul style="list-style-type: none"> ● 2400 g
Dimensions	<ul style="list-style-type: none"> ● 442 x 170 x 44 mm

7

Network Glossary

The network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

100Base-FX

The IEEE standard defines how to transmit Fast Ethernet 100Mbps data using multi-mode or single fiber optic cable

100Base-TX

Also known as 802.3u. The IEEE standard defines how to transmit Fast Ethernet 100Mbps using Cat.5 UTP/STP cable. The 100Base-TX standard is backward compatible with the 10Mbps 10-BaseT standard.

1000Base-SX

Also known as 802.3z. The IEEE standard defines how to transmit gigabit Ethernet data using multi-mode fiber optic cables. This standard allows transmission distance of 550 meter, which is more than 5 times longer than the 100-meter limitation of 1000Base-T. The 1000Base-SX cannot run in 100Mbps mode.

1000Base-LX

The IEEE standard defines how to transmit gigabit Ethernet data using single mode fiber optic cables. This standard allows transmission distance of 5km or more using single mode fiber. The 1000Base-LX cannot run in 100Mbps mode.

1000Base-T

Also known 802.3ab standard. The IEEE standard defines how to transmit Gigabit data

through the use of Cat.5 UTP/STP cable. The 1000Base-T can run in 10/100/1000Mbps speed, and is backward compatible with 10/100Base-TX standard.

802.1d STP

Spanning Tree Protocol. It is an algorithm to prevent network from loop topology. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loop must be avoided because of flooding issue in the network.

802.1Q Tag VLAN

In 802.1Q VLAN, the VLAN information is written into the Ethernet packet itself. Each packet carries a VLAN ID(called Tag) as it traveled across the network. Therefore, the VLAN configuration can be configured across multiple switches. In 802.1Q spec, possible 4096 VLAN ID can be created. Although for some devices, they can only view in frames of 256 ID at a time.

802.1x

802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

802.1w

Rapid Spanning Tree Protocol. It is a refinement of STP, which provides faster spanning tree convergence after a topology change. While STP can take 30 or 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

DHCP

Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned by DHCP server. A DHCP server can either be a

designed PC on the network or another network device, such as a router.

Firmware

The program that runs inside embedded device such as AP or Switch. Many network devices are firmware upgradeable through web interface or utility program.

FTP

File Transfer Protocol. A standard protocol for sending files between computer over a TCP/IP network and the internet.

IGMP Snooping

Internet Group Management Protocol. It is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP Snooping is a feature that allows an Ethernet Switch to “listen in” on the IGMP conversation between hosts and routers. When IGMP snooping is enabled in a switch, it prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (IGMP client).

IP Address

IP (Internet Protocol) is a Layer 3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

LACP (802.3ad) Trunking

Link Aggregation Control Protocol. It is protocol defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both devices must set the trunking feature to work.

MAC

Media Access Control. MAC address provides Layer-2 identification for network devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each device manufacturers. When a network device has MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps

Megabits Per Second. One million bits per second; a unit of measurement for data transmission.

MiniGBIC

A type of Gigabit Ethernet module interface that uses SFP (Small Form-factor Pluggable) transceiver. The MiniGBIC equipped with Switches typically comes with the MiniGBIC slot for optional SFP optical transceiver.

Packet

A unit of data sent over a network.

Rate Control

It is an Ethernet switch's function to control the upstream and downstream speed of an individual port. Rate control management use "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. The SNMP network contains three key elements: managed devices, agents, and network-management system (NMS). Managed devices are network devices that contain SNMP agents. SNMP agents are programs that reside SNMP capable device's firmware to provide SNMP configuration service. The NMS typically is PC-based software that can monitor and control managed devices remotely.

Subnet Mask

An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

TFTP

Trivial File transfer Protocol. A file transfer protocol, with the functionality of a very basic form of FTP. It is used to transfer small amounts of data between hosts on a network, such as Switch firmware.